NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

Időbélyegzés Szolgáltatási Rend (ISZR)

Ferencz Attila József

Digitálisan aláírta: Ferencz Attila József
DN: c=HU, l=Budapest, o=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., title=igazgató, serialNumber=DO20130917-1DO27, cn=Ferencz Attila József, postalCode=1081, street=Csokonai utca 3.
Dátum: 2016.04.15 14:56:47 +02'00'

Verziószám	**1.2**
OID szám	**0.2.216.1.200.1100.100.42.3.3.6.1.2**
Hatósági azonosító jel	**NI-16041501-IR**
Hatályba lépés dátuma	**2016.05.15.**
Dokumentum besorolása	**Publikus**

NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

Változáskövetés

Ver-zió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2013.08.14	Első változat	Lencse Zsolt Kővári Ferenc	Nagy András	
1.1	2014.02.07.	Hatóság észrevételei alapján módosított változat	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila
1.2	2016.04.15.	Állandó személyazonosító igazolványhoz (eSZIG) kapcsolódó időbélyegzés szolgáltatás nyújtása miatt bővített változat	Kővári Ferenc	dr. Sandl Judit	Ferencz Attila

TARTALOMJEGYZÉK

1. Bevezetés

Jelen dokumentum a NISZ Zrt. elektronikus aláírással kapcsolatos szolgáltatásaihoz tartozó Időbélyegzés Szolgáltatási Rend (továbbiakban: ISZR).

A NISZ Zrt. (továbbiakban: Szolgáltató) jelen ISZR-ben szabályozott időbélyegzés szolgáltatását a 2001. évi XXXV. számú, elektronikus aláírásról szóló törvény (továbbiakban Eat.) 6.§-ban meghatározott időbélyegzés szolgáltatásként kell értelmezni (továbbiakban még: Szolgáltatás).

A NISZ Zrt. jelen ISZR-hez kapcsolódó időbélyegzés szolgáltatását az Eat. szerinti minősített szolgáltatóként nyújtja.

A Szolgáltató által kiadott időbélyeg hozzákapcsolható mind fokozott biztonságú, mind minősített aláírással ellátott dokumentumokhoz, valamint elektronikusan alá nem írt állományokhoz is.

Jelen Időbélyegzési Szolgáltatási Rend hatálya alatt a Szolgáltató az időbélyegzés szolgáltatást két ügyfélcsoport részére nyújtja:

a) a 84/2012. Korm. rendelet 7/C. § pontja szerinti kijelölés alapján, azon állampolgárok számára, akik az elektronikus tároló elemmel ellátott állandó személyazonosító igazolványuk e-aláírás funkciójához kapcsolódó szolgáltatások igénybevételére szolgáltatási szerződést kötöttek (továbbiakban: eSZIG ügyfelek);

b) a 84/2012. Korm. rendelet 4. § g) pontja szerinti kormányzati hitelesítés-szolgáltatás keretében, jogi személy vagy jogi személyiség nélküli szervezetek számára (továbbiakban: közületi ügyfelek)

Jelen Időbélyegzés Szolgáltatási Rend meghatározza az időbélyegzés szolgáltatás szereplőit, azok feladatait, kötelezettségeit és felelősségét, a Szolgáltató működésére vonatkozó követelményeket, valamint az időbélyegzés szolgáltatás menedzsment és az időbélyegzéshez tartozó kulcsmenedzsment életciklusára vonatkozó szabályokat.

2. Az ISZR hatálya

Jelen ISZR tárgyi hatálya a Szolgáltató minősített időbélyegzés szolgáltatására, valamint az ezzel kapcsolatban álló összes objektumára, tárgyi eszközére terjed ki.

Az ISZR időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik, és határozatlan időre szól. Időbeli hatálya megszűnik egy újabb ISZR verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor. Az ISZR módosítását a vonatkozó jogszabályok szerint 30 nappal előzetesen be kell jelenteni az illetékes hatóság (Nemzeti Média- és Hírközlési Hatóság - NMHH) részére nyilvántartásba vétel céljából.

Az ISZR személyi hatálya a Szolgáltatóra, annak a szolgáltatásban közreműködő munkatársaira, valamint a felhasználói közösségre (Előfizetők és felhasználók, illetve az Érintett felek) terjed ki.

3. Jogszabályi és szabályzati megfelelés

Jelen ISZR-hez kapcsolódó minősített időbélyegzés szolgáltatás, valamint a Szolgáltató ezzel kapcsolatos tevékenysége megfelel az elektronikus aláírásról szóló 2001. évi XXXV. törvénynek, az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendeletnek, a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV.26) MeHVM irányelvnek[1], az RFC3161 ajánlásnak, valamint az időbélyegzés szolgáltatókra vonatkozó követelményekről szóló ETSI TS 102 023 szabványnak.

Ezen túlmenően a jelen ISZR összhangban van a NISZ Zrt. belső szabályzataival, ezen belül a PKI szolgáltatásokra vonatkozó üzemeltetési és biztonsági szabályzatokkal.

4. Általános rendelkezések

4.1. Az időbélyegzés szolgáltatás komponensei

Az időbélyegzés szolgáltatás keretében Szolgáltatónak a következő tevékenységeket kell végeznie:

a. időbélyeg előállítás, melynek során Szolgáltató időbélyegeket állít elő és bocsát ki az Előfizetők részére

[1] A 2/2002 MeHVM nem hatályos jogszabály, de az aktuális részeit Szolgáltató ajánlásként figyelembe veszi

b. időbélyegzés menedzsment, melynek során Szolgáltató biztosítja az időbélyeg előállítás megbízható működését, és ellenőrzi az időbélyegzés szolgáltatás megfelelőségét a vonatkozó követelmények alapján.

Ennek megfelelően Szolgáltató informatikai rendszere két fő összetevőből kell álljon:

a. az időbélyegeket előállító és kibocsátó egységek,

b. az időbélyegeket előállító és kibocsátó egységek megbízható működését felügyelő és menedzselő alrendszer, amely a következő funkciókat látja el:

- felügyeli az időbélyegző szerverek működését, kiesés esetén irányítja az áttérést a meleg tartalék szerverre,
- biztosítja az időbélyegző szerverek belső időszinkronját,
- biztosítja a belső időszinkronizálást végző óra legalább két egymástól független UTC[2] időalappal történő időszinkronizálását,
- figyeli az időbélyegző szerver belső órájának a pontossági tartományból való kilépését, ennek bekövetkezés esetén kezdeményezi a szolgáltatás leállítását és a hibaüzenet kiadását az üzemeltetők felé,
- támogatja az installációs, a karbantartási, a naplózási, az archiválási, a mentési és a leállítási műveleteket.

4.2. Időbélyegzés szolgáltató

A jelen dokumentumban meghatározott időbélyegzés szolgáltatást a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (Szolgáltató) nyújtja.

A Szolgáltató általános adatait, valamint a Szolgáltatásért illetékes szervezetnek (Ügyfélkapcsolati Irodának) az elérhetőségét, nyitva tartását, a Szolgáltatóval való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a NISZ Zrt. „Szolgáltatási Szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz” c. szabályzata (HSZSZ-M) tartalmazza.

4.3. Előfizetők és felhasználók. Érintett felek

A Szolgáltató az időbélyegzés szolgáltatást a vele szerződéses viszonyban álló Előfizetők illetve a velük kapcsolatban álló felhasználók (végfelhasználók) részére nyújtja.

a) közületi ügyfelek esetén Előfizető bármely Európai Unióban bejegyzett cég illetve szervezet (jogi személy), amely a Szolgáltatóval időbélyegzés szolgáltatásra szerződést köt, a NISZ Zrt. „Általános Szerződési Feltételek a PKI szolgáltatásokhoz” című dokumentuma (továbbiakban: ÁSZF-PKI) szerint.

b) eSZIG esetén Előfizetők az időbélyegzés szolgáltatást igénybe vevő, a Szolgáltatóval szerződéses viszonyban álló eSZIG tulajdonosok (állampolgárok). A szerződési feltételeket a NISZ Zrt. „Általános Szerződési Feltételek a PKI szolgáltatásokhoz” című dokumentuma (továbbiakban: ÁSZF-PKI) tartalmazza

Közületi ügyfelek esetén Előfizető mint jogi személy felelős a vele kapcsolatban álló felhasználók tájékoztatásáért valamint a rájuk vonatkozó szabályok betartásáért.

A Szolgáltató által kiadott időbélyegek az Előfizetőkön (illetve végfelhasználóikon) túl eljuthatnak egyéb felhasználókhoz is, akik (ha természetes személyek) vagy amelyek (ha jogi személyek) az időbélyegre hagyatkozva járnak el, de nem állnak szerződéses jogviszonyban Szolgáltatóval (a továbbiakban: Érintett felek).

4.4. Az Időbélyegzés Szolgáltatási Rend és a szolgáltatási szabályzat kapcsolata

Jelen ISZR a Szolgáltatóra, az általa nyújtott időbélyegzés szolgáltatásra, valamint az azt támogató informatikai rendszerre vonatkozóan általános követelményeket és szabályokat határozza meg.

A Szolgáltatónak rendelkeznie kell olyan szolgáltatási szabályzattal, melyben leírja, hogy ezen általános követelményeket milyen módon és milyen konkrét megoldásokat alkalmazva teljesíti a gyakorlatban[3].

[2] UTC: Coordinated Universal Time, az ITU-R TF.460-5 ajánlás szerint definiált, másodperc felbontású időalap.

[3] NISZ Zrt. Szolgáltatási Szabályzat a minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M).

5. Időbélyegzés politika

5.1. Áttekintés

eSZIG ügyfelek esetén

Az időbélyegzés szolgáltatást azok az állampolgárok vehetik igénybe, akik az elektronikus tároló elemmel ellátott állandó személyazonosító igazolványuk e-aláírás funkciójához kapcsolódó szolgáltatások igénybe vételére (beleértve az időbélyegzés szolgáltatást is) szolgáltatási szerződést kötöttek.

Az időbélyegzési kérelem elfogadása során Szolgáltató olyan eljárást kell alkalmazzon, amellyel megállapítja Előfizető eSZIG-hez kapcsolódó jogosultságát Ennek részleteit Szolgáltató a vonatkozó szolgáltatási szabályzatában meg kell határozza.

Az időbélyegek szerkezetére és tartalmára vonatkozóan Szolgáltatónak az ETSI TS 101 861 szabvány előírásait kell alkalmaznia. Az időbélyegeknek tartalmazniuk kell a jelen ISZR objektum azonosítóját (OID) és az időbélyeg kibocsátás pontosságát. Az időbélyegeket a Szolgáltatónak saját maga által kibocsátott tanúsítványon alapuló elektronikus aláírással kell hitelesítenie.

Közületi ügyfelek esetében

Az időbélyegzés szolgáltatást igénybe veheti a Szolgáltatóval szerződéses viszonyban álló bármely Előfizető, függetlenül attól, hogy részére az elektronikus aláírás hitelesítés-szolgáltatást a NISZ Zrt. vagy más hitelesítés szolgáltató nyújtja.

Az időbélyegzési folyamat során a Szolgáltató és az időbélyegzés felhasználó közötti kommunikáció protokolljára vonatkozóan Szolgáltatónak be kell tartania az IETF RFC 3161 szabvány előírásait; az időbélyegzést támogató szolgáltatói alkalmazásra, valamint az időbélyegek szerkezetére és tartalmára vonatkozóan pedig az ETSI TS 101 861 szabvány előírásait kell alkalmaznia. Az időbélyegeknek tartalmazniuk kell a jelen ISZR objektum azonosítóját (OID) és az időbélyeg kibocsátás pontosságát. Az időbélyegeket a Szolgáltatónak saját maga által kibocsátott tanúsítványon alapuló elektronikus aláírással kell hitelesítenie.

5.2. Az ISZR azonosítása

Jelen dokumentum teljes neve: Időbélyegzés Szolgáltatási Rend

Jelen dokumentum rövid neve: ISZR

A dokumentum azonosítója (OID) és verziószáma a dokumentum címlapján található.

A dokumentum hatósági azonosító jele szintén a címlapon található.

Az ISZR publikus dokumentum, aktuális verziója letölthető a Szolgáltatás internetes honlapjáról (http://hiteles.gov.hu).

Jelen ISZR-nek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

5.3. Felhasználó közösség és alkalmazhatóság

Az időbélyegzés szolgáltatást minden, a 4.3 pontban meghatározott Előfizető illetve végfelhasználója igénybe veheti, függetlenül attól, hogy az időbélyeget nyilvános vagy zárt körben használja.

5.4. Megfelelés

A Szolgáltatónak meg kell felelnie a hatályos jogszabályi előírásoknak, továbbá a szolgáltatásra vonatkozó hazai valamint nemzetközi szabványoknak és ajánlásoknak (ld. 3. pont). A megfelelést független belső és külső auditorok által rendszeresen elvégzett vizsgálatokkal kell biztosítani.

6. Kötelezettségek és felelősségek

6.1. A Szolgáltató kötelezettségei

6.1.1. Általános kötelezettségek

A Szolgáltató alapvető kötelezettsége, hogy az időbélyegzés szolgáltatását a vonatkozó jogszabályoknak, szabványoknak és ajánlásoknak, továbbá a hitelesítés szolgáltatási szabályzatának (HSZSZ-M) megfelelően nyújtsa, és ennek során érvényesítse a jelen ISZR előírásait, valamint az előfizetői szerződésben valamint az általános szerződési feltételekben (ÁSZF-PKI) leírtakat.

6.1.2. Kötelezettségek az Előfizetővel és a felhasználókkal szemben

A Szolgáltató a következőkre vállal kötelezettséget az Előfizetők illetve a felhasználók felé:

a. a felhasználótól érkező szabványos időbélyeg kérésekre szabványos[4] időbélyeget bocsájt ki,

b. biztosítja, hogy a kiadott időbélyeg - az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve - ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott,

c. nem ismeri meg az időbélyeggel ellátott dokumentum tartalmát

d. a kibocsátott időbélyeg nem tartalmaz hibás adatot,

e. időbélyeget aláíró szolgáltatói kulcsot csak az időbélyegzés keretén belül használja,

f. az időbélyeget 1 másodpercen belüli pontossággal adja ki,

g. az időbélyegzési rendszer belső óráját 0,1 másodperc pontossággal szinkronizálja az UTC időalaphoz.

h. az időbélyegzés szolgáltatás biztonságát a minősített hitelesítés szolgáltatókra vonatkozó követelmények szerint biztosítja,

i. rögzít az időbélyegzéssel kapcsolatos minden fontos eseményt, ezeket naplózza és a napló állományokat biztonságosan archiválja.

6.2. Az Előfizetők illetve a felhasználók kötelezettségei

Az Előfizető kötelezettségeit a Szolgáltatóval megkötött előfizetői szerződés, továbbá a Szolgáltató hitelesítés szolgáltatási szabályzata (HSZSZ-M) és általános szerződési feltételei (ÁSZF-PKI) tartalmazzák. Előfizetők végfelhasználóinak feladata a kért időbélyeg vétele után meggyőződni az időbélyegen szereplő aláírás helyességéről és az aláíró kulcshoz tartozó szolgáltatói tanúsítvány érvényességéről és státuszáról a visszavont tanúsítványok listájának segítségével. Ennek módját részletesen a HSZSZ-M 2.1.3 pontja tartalmazza.

6.3. Az Érintett félre vonatkozó ajánlás

Egy időbélyeggel ellátott állomány fogadásakor az Érintett félnek a tőle elvárható gondosság érdekében javasolt ellenőriznie az időbélyegen szereplő aláírás helyességét és az aláíró kulcshoz tartozó szolgáltatói tanúsítvány érvényességét és státuszát a visszavont tanúsítványok listájának segítségével, a HSZSZ-M 2.1.3 pontjában leírt módon.

6.4. Felelősség

Szolgáltató felelősségére és a saját hibájából adódó kár megtérítésére vonatkozóan a HSZSZ-M 2.2.1. pontja vonatkozik.

7. A Szolgáltató működési követelményei

7.1. Szolgáltatási és a közzétételi szabályozás

7.1.1. Időbélyegzés szolgáltatás szabályozása

Az időbélyegzés szolgáltatást a NISZ Zrt. egy olyan időbélyegző informatikai alrendszerrel kell biztosítsa, amely a minősített elektronikus aláírás hitelesítést szolgáltató informatikai rendszerrel közös fizikai környezetben működik.

Az időbélyegzés szolgáltatást a Szolgáltató folyamatosan (az év minden napján, 24 órában), 99,9%-os rendelkezésre állással kell biztosítsa úgy, hogy a szolgáltatás kiesése esetenként nem lépheti túl a 3 órás időtartamot.

A NISZ Zrt. minősített szolgáltatóként nyújtja az időbélyegzés szolgáltatást, így az időbélyegző informatikai alrendszer, annak fizikai és személyi környezete meg kell feleljen a minősített szolgáltatókra vonatkozó követelményeknek. A megfelelést biztosító technikai, működtetési, menedzselési és biztonsági megoldásokat és szabályokat a NISZ Zrt. HSZSZ-M szabályzata rögzíti. A HSZSZ-M megfelelő pontjai tartalmazzák az időbélyegzés szolgáltatás következő vonatkozásait is:

- Szolgáltató és felhasználó közösség, alkalmazhatóság (HSZSZ-M 1.3 és 1.4 pont),

[4] (IETF RFC 3161 és ETSI TS 101 861)

- Feladatok és hatáskörök (HSZSZ-M 2.1 pont),
- A szolgáltató és felhasználó közösség tagjainak felelőssége (HSZSZ-M 2.2 pont),
- Az anyagi felelősség mértéke (HSZSZ-M 9.2 pont),
- Irányadó jog (HSZSZ-M 2.3.1 és 10.5 pont),
- Érvénytelenség, hatályosság, megszűnés, értesítések (HSZSZ-M 2.4.2 pont),
- Közzététel (HSZSZ-M 2.4 pont),
- A megfelelőség vizsgálata (HSZSZ-M 8 pont),
- Azonosítás és hitelesítés (HSZSZ-M 3. pont),
- A működésre vonatkozó követelmények (HSZSZ-M 4. pont),
- Biztonsági audit eljárások (HSZSZ-M 8. pont),
- Adatarchiválás (HSZSZ-M 5.5 pont),
- A folyamatos üzemmenet biztosítása (katasztrófa elhárítás) (HSZSZ-M 5.8 pont),
- Szolgáltatási tevékenység megszüntetése (HSZSZ-M 5.9 pont),
- Fizikai, eljárásrendi, és humán biztonsági szabályozások (HSZSZ-M 5. pont),
- Kulcspár előállítás (HSZSZ-M 6.1.1 pont),
- Aláírás-létrehozó adat védelme (HSZSZ-M 6.2 pont),
- Számítógép biztonsági szabályok (HSZSZ-M 6.6 pont),
- Életciklus technikai szabályok (HSZSZ-M 6.7 pont),
- Kriptográfiai modul ellenőrzése (HSZSZ-M 6.9 pont),
- Tanúsítvány és kulcs-visszavonási profil (HSZSZ-M 7. pont).

7.1.2. Közzétételi nyilatkozat

Az ETSI TS 102 023 szabvány 7.1 pontja szerint a Szolgáltatónak az időbélyegzés szolgáltatás használatával kapcsolatos információkat és feltételeket tartalmazó közzétételi nyilatkozatot kell nyilvánosan elérhetővé tennie.

Ennek megfelelően Szolgáltató az alábbi nyilatkozatot teszi közzé, amely a Szolgáltatás internetes honlapján keresztül érhető el.

A szabály megnevezése	A szabály kifejtése
Időbélyegzés szolgáltatás szabályozása	Időbélyegzés szolgáltatás részletes szabályait a NISZ Zrt. „Szolgáltatási Szabályzat minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz” című dokumentuma (HSZSZ-M) tartalmazza.
A Szolgáltató elérhetősége	**NISZ Nemzeti Infokommunikációs Szolgáltató Zrt**. Cégjegyzék szám: Cg. 01-10-041633- Székhely: 1081 Budapest, Csokonai u. 3. Levélcím: 1389 Budapest, Pf.: 133. Telefonszám: (36-1) 459-4200 Telefax szám: (36-1) 303-1000 Internetes honlap címe: *http://www.nisz.hu/* Szolgáltatás internetes honlapja: *http://hiteles.gov.hu* **Szolgáltatásért felelős szervezeti egység: PKI Ügyfélkapcsolati Iroda** Cím:1081 Budapest, Csokonai u. 3. Telefon: +36-1-795-7200 és +36-30-795-7200 Fax: +36-1-795-0100 E-mail: info@hiteles.gov.hu

A szabály megnevezése	A szabály kifejtése
	Illetékes ügyfélszolgálat (7/24) eSZIG esetén: Telefon: 1818 (Kormányzati Ügyfélvonal), külföldről: +36 1 550-1858 Email: 1818@1818.hu **NISZ illetékes ügyfélszolgálata (7/24) közületi ügyfelek esetén:** Telefon: +36 1 795-7300 és +36 30 795-7300 E-mail: smc@nisz.hu **Panaszok bejelentésének helye és módja eSZIG esetén:** Az időbélyegzés szolgáltatást igénybe vevő eSZIG tulajdonosok a Kormányzati Ügyfélvonal 1818 hívószámán telefonon vagy emailben a 1818@1818.hu címre küldve, továbbá írásban a Kormányzati Ügyfélvonalhoz címezve a 1476 Budapest, Pf: 281 postacímre terjeszthetik elő a panaszt Szolgáltató részére **Panaszok bejelentésének helye és módja közületi ügyfelek esetén**: Személyesen a PKI Ügyfélkapcsolati Irodán, Írásban a Szolgáltató levélcímére címezve, Telefonon és faxon a PKI Ügyfélkapcsolati Irodán Elektronikus levélben a PKI Ügyfélkapcsolati Iroda e-mail címére. **Illetékes fogyasztóvédelmi felügyelőség:** Budapest Főváros Kormányhivatala, Fogyasztóvédelmi osztály 1052 Budapest, Városház u. 7. Telefon: 450 2598 Email: fogyved_kmf_budapest@nfh.hu
ISZR azonosító (OID)	**0.2.216.1.200.1100.100.42.3.3.6.2**
Alkalmazható lenyomatképző algoritmus	a Nemzeti Média- és Hírközlési Hatóság 2011. évben erre vonatkozóan kiadott határozatának 1. sz. melléklete szerinti SHA-256
Az időbélyegben szereplő idő pontossága	Összhangban a 2/2002. (IV.26) MeHVM irányelv 219. pontjával, az UTC-vel szinkronizált idő pontossága: 1 másodpercen belül van.
Az időbélyegzés alkalmazhatóságának korlátjai	**<u>eSZIG esetén</u>** Az elektronikus tároló elemmel rendelkező személyazonosító igazolványokhoz (eSZIG) kapcsolódó időbélyegzés szolgáltatást az ügyfelek csak az eSZIG-gel történő elektronikus aláíráshoz kapcsolódóan jogosultak igénybe venni, magánemberként illetve állampolgárként. A szolgáltatás használata bármilyen üzleti, munkahelyi vagy ilyen jellegű szakmai tevékenység céljából nem megengedett A szolgáltatás igénybevételéhez olyan alkalmazást kell használni, amely biztosítja, hogy az időbélyeg kérés a beküldés előtt az eSZIG-en tárolt minősített tanúsítványhoz kapcsolódó magánkulccsal aláírásra kerül. A szolgáltatás keretében igényelhető időbélyegek számát Szolgáltató jogosult korlátozni; az erre vonatkozó részleteket a vonatkozó szolgáltatási szabályzat (HSZSZ-M) tartalmazza. **<u>Közületi ügyfelek esetében</u>** Előfizető az Európai Unióban bejegyzett cég vagy jogi személyiséggel rendelkező szervezet. Az időbélyegzés szolgáltatás igénybevételéhez érvényes, Szolgáltató által kibocsátott, azonosításra alkalmas tanúsítvány vagy egyéb, a Szolgáltatótól származó és az Előfizető egyértelmű azonosítását lehetővé tevő adat (pl. felhasználónév és

A szabály megnevezése	A szabály kifejtése
	jelszó) szükséges.
Az időbélyeg ellenőrzés módja	Egy időbélyeggel ellátott állomány elfogadása során indokolt meggyőződni az időbélyeg aláírásának helyességéről és a szolgáltatói aláíró kulcs tanúsítványának érvényességéről a HSZSZ-M 2.1.3 pontjában leírt módon.
Időbélyegző rendszer naplók archiválási időtartama	A 3/2005. (III. 18.) IHM. rendelettel összhangban az archivált naplókat keletkezésüktől számított 10 évig, illetőleg a velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrződnek.
Hatályos jogszabályok az időbélyegzés vonatkozásában	♦ 2001. évi XXXV. törvény az elektronikus aláírásról. ♦ 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről. ♦ 2/2002. (IV.26) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.* ♦ az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény ♦ 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról. ♦ 1992. évi LXVI törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról ♦ 84/2012. (IV.21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről * A 2/2002 (IV.26) MeHVM irányelv nem hatályos jogszabály, de az aktuális részeit Szolgáltató ajánlásként figyelembe veszi
A Szolgáltató felelősségének korlátozása	A Szolgáltató felelősségéből adódó kár megtérítésére vonatkozóan az ÁSZF-PKI 5.1.3 pontja érvényes.
Eljárás jogi viták rendezésére	A jogi viták rendezésére az ÁSZF-PKI 9. pontja érvényes
Nyilvántartásba vételi eljárásért illetékes hatóság	Nemzeti Média- és Hírközlési Hatóság

7.2. A kulcsmenedzsment életciklusa

7.2.1. A szolgáltatói kulcspár generálása

A Szolgáltató maga kell előállítsa az időbélyegző egységek szolgáltatói kulcspárjait (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben, kriptográfiai modulban (HSM[5]). A kriptográfiai modulnak rendelkeznie kell a 9/2005. (VII. 21.) IHM rendelet szerint kijelölt szervezet vagy ezzel egyenértékű Európai Uniós szervezet által kiadott tanúsítással, illetve szerepelnie kell a Nemzeti Média- és Hírközlési Hatóság által nyilvántartott minősített elektronikus aláírási termékek listájában.

A kulcspár előállítás fizikai védelme és személyi környezete meg kell feleljen a minősített szolgáltatókra vonatkozó követelményeknek.

7.2.2. Az időbélyegző egységek kulcsainak védelme

Az időbélyegző egységek aláíró kulcsának védelme a 7.2.1. pontban körülírt kriptográfiai modul (HSM) felhasználásával kell történjen.

[5] Hardware Security Module

Az időbélyegző egységek aláíró kulcsának fizikai védelme és személyi környezete meg kell feleljen a minősített hitelesítés szolgáltatókra vonatkozó követelményeknek.

7.2.3. Az időbélyegző egységek nyilvános kulcsainak közzététele

Az időbélyegző egységek nyilvános kulcsai és tanúsítványai a Szolgáltatás internetes honlapján keresztül elérhetők kell legyenek.

7.2.4. Az időbélyegző egységek kulcsainak megújítása

Az időbélyegző egységek kulcsainak megújítása a tanúsítványuk érvényességi idejének lejártakor történik, hacsak addig a kulcs nem kompromittálódott. A kulcs megújítás szabályait részletesen a minősített HSZSZ-M 6 pontja, a kompromittálódás elkerülésére foganatosított, illetve a bekövetkezés esetén megvalósítandó intézkedéseket részletesen a HSZSZ-M 5.8 pontja és a PKI Szolgáltatások Üzletmenet-folytonossági Terve tartalmazza.

7.2.5. Az időbélyegző egységek kulcsmenedzsment életciklusának vége

Az időbélyegző egységek kulcsmenedzsment életciklusa a következő esetekben fejeződik be:

1. a kulcs és tanúsítványának érvényességi ideje lejár,
2. a kulcs kompromittálódik,
3. katasztrófa esemény vagy a Főtanúsítványkiadó (Root CA) illetve a Minősített Tanúsítványkiadó aláíró kulcs kompromittálódása miatt a Szolgáltatás befejeződik.
4. új CA hierarchiára való átállás miatt, vagy új TSA hierarchiára való átállás miatt

Az 1. esetben a kulcs megújításra kerül a 7.2.4. pont szerint.

A 2. és 3. esetben a tanúsítványt azonnal vissza kell vonni és az aláíró kulcsot meg kell semmisíteni.

A 4. esetben amennyiben szükséges, új kulcsot kell generálni és hitelesíteni, a régi visszavonását amint lehet, meg kell valósítani.

7.2.6. Az időbélyegek aláírásához használt kriptográfiai modulok életciklus menedzsmentje

A jelen ISZR 7.1.1. illetve 7.2.2 pontjában meghatározott kriptográfiai modulok (HSM) a Szolgáltató fizikailag védett központi géptermében, külön erre a célra kijelölt bizalmi munkaköröket betöltő személyekből felállított bizottság előtt kerülnek installálásra és üzembe helyezésre. A bizottság az üzembe helyezés előtt ellenőrizte a hardver modulok sértetlenségét.
A kriptográfiai modulok üzemeltetése a Szolgáltató központi géptermében történik a minősített szolgáltatás követelményeinek megfelelő körülményekben és személyzet által.

Az időbélyegek aláírásához használt kriptográfiai modul rendszerből történő kivonása esetén az aláíró kulcsot bizottság előtt jegyzőkönyv felvétele mellett meg kell semmisíteni.

7.3. Időbélyegzés

Az időbélyeg felépítése meg kell feleljen az IETF RFC 3161 szabványnak és a jelen ISZR-ben meghatározott egyéb követelményeknek a következők szerint:

- tartalmazza az 5.2 pontban meghatározott ISZR azonosítót,
- tartalmazza az időbélyeg egyedi azonosítóját,
- Az időbélyegben megadott időpontot az időbélyegzés szolgáltató belső rendszere adja, amelyet legalább 2, egymástól független, az UTC idővel szinkronizált időforrásnak kell kiszolgálnia. Ennek során a Szolgáltatónak garantálnia kell, hogy belső óráját 0,1 másodperces pontossággal szinkronizálja az UTC időalaphoz, és a kibocsátott időbélyegek pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól.
- a HSZSZ-M 6.5 pontjában részletesen ismertetett belső és külső szinkronizáló eljárást kell biztosítani;
- a külső szinkron tartalékolt, az egyes órajelek esetleges manipulációját belső kontroll szűri ki;
- a belső órajel hitelességét az időbélyegző alrendszer indításakor egy erre a célra összehívott bizottság tanúsítja;
- üzemközben a belső óra hitelességét a redundáns külső UTC időalapokkal a bizottság által történő összevetés és egy a rendszertől független GPS kapcsolaton keresztül történő, referenciaként használt UTC időlekérdezés biztosítja,

- a Szolgáltató által visszaküldött időbélyeg a kérelmező üzenete által meghatározott adatokat tartalmazza;
- a kérelem része az időbélyeggel ellátandó adat lenyomata is;
- a Szolgáltató az időbélyeget csak az időbélyegzés céljára kiadott aláíró kulccsal írja alá
- Az időbélyegben az aláírásra használt szolgáltatói kulcsot a Szolgáltató más célra nem használja
- az időbélyeg egy olyan Szolgáltatói névmegadást tartalmaz, amely tartalmazza:
  - a Szolgáltató országának nevét (C),
  - a Szolgáltató és az időbélyegző szerver azonosítóját (CN),
  - az időbélyeget kibocsátó szervezet nevét (O),
  - az időbélyeget kibocsátó szervezet székhelyét (város) (L)

7.3.1. Óraszinkronizálás az UTC-vel

Az időbélyegző alrendszer belső órájának a pontossági tartományon belül maradását a belső és külső szinkronizációs eljárás biztosítja.

A Szolgáltató az UTC-hez szinkronizálja az időbélyegzés szolgáltatás során használt belső óráját és garantálja, hogy a legnagyobb eltérés az UTC-től nem haladhatja meg a 0,1 másodpercet.

A külső szinkronizálást két egymástól független UTC időalap támogatja, amelyekkel nagy megbízhatósággal biztosítható az időbélyegzés belső órájának pontossága, valamint a külső órajelek redundancián alapuló ellenőrzésével annak hitelessége is.

Az időbélyegzés belső órájának pontossága folyamatos ellenőrzés alatt áll. Amennyiben a nagy megbízhatóságú időszinkronizálás ellenére a belső óra pontossága az előírt 1 másodperces tartományból kiesne, az időbélyegzés szolgáltatás leáll, és a hiba kijavításáig minden további kérésre hiba üzenetet küld az Előfizetők felé.

A Szolgáltatás az időbélyegző szerverek belső órái által helyesen vett időszinkronnal indul.

A Szolgáltató a fenti szinkronizációs és ellenőrzési mechanizmusokkal biztosítja a 2/2002. (IV.26) MeHVM irányelv 219. pontjának való megfelelőséget.

Az időbélyegző alrendszer fizikai védelme fokozott szinten biztosított, mert abban a gépteremben került elhelyezésre, amelyben a minősített hitelesítés szolgáltató rendszer is üzemel.

7.4. Időbélyegzés szolgáltatás menedzsment és működtetés

7.4.1. Biztonságmenedzsment

Szolgáltatónak az időbélyegzés szolgáltatást biztonságos fizikai, szabályozási és személyi környezetben kell nyújtania. Az időbélyegzés szolgáltatói rendszernek, valamint a Szolgáltatás fizikai, szabályozási és személyzeti környezetének meg kell felelnie a jogszabályok által előírt, minősített szolgáltatókra vonatkozó követelményeknek..

A részletes biztonsági intézkedéseket egyrészt a Szolgáltató HSZSZ-M szabályzata, másrészt a belső használatú szabályzatai tartalmazzák.

A biztonságmenedzsment szabályozási hátterét képezik:

a. a PKI Szolgáltatások Informatikai Biztonságpolitikája,
b. a PKI Szolgáltatások Biztonsági Szabályzata,
c. a PKI Szolgáltatások Üzletmenet-folytonossági Terve.

7.4.2. Az eszközök biztonsági osztályba sorolása és menedzsmentje

A PKI Szolgáltatások Informatikai Biztonságpolitikája szerint az időbélyegzést támogató informatikai alrendszer biztonsági osztályba sorolása az elvégzett kockázatelemzés után a következő:

Információvédelem szempontjából	FOKOZOTT BIZTONSÁGI OSZTÁLY

Megbízható működés szempontjából	KIEMELT BIZTONSÁGI OSZTÁLY

Ez megfelel a MeH ITB 12. ajánlás és az ITSEC szerinti biztonsági osztályba sorolásnak.

A minősített szolgáltató rendszerre, annak fizikai és személyi környezetére vonatkozó biztonsági követelményeket a Szolgáltató egyik belső (nem publikus) dokumentuma tartalmazza.

Ennek, valamint a 3/2005. (III. 18.) IHM. rendeletnek és a 2/2002. (IV.26) MeHVM irányelv 212. pontjának megfelelően a NISZ Zrt.-n belül megtörtént a teljes szolgáltató rendszernek, illetve a fizikai és személyi környezetének kockázatelemzés alapú vizsgálata.

A NISZ Zrt. PKI biztonságpolitikájának és szabályzatának, valamint a PKI Változásmenedzsment Szabályzatának megfelelően az időbélyegzés szolgáltatást támogató informatikai rendszer hardver és szoftver elemei leltárba lettek véve, amelynek a karbantartása változásmenedzsment keretében valósul meg.

7.4.3. Személyzeti biztonság

A Szolgáltató rendszerének személyzeti biztonsági követelményei meg kell feleljenek a minősített szolgáltatókra vonatkozó követelményeknek.

A személyi biztonság követelményeinek való megfelelést részletesen a HSZSZ-M tartalmazza.

7.4.4. A fizikai infrastruktúra biztonsága

A fizikai infrastruktúra biztonsága meg kell feleljen a minősített szolgáltatókra vonatkozó követelményeknek.

A követelményeinek való megfelelést részletesen a HSZSZ-M tartalmazza.

7.4.5. Üzemeltetés menedzsment

A Szolgáltató üzemeltetési tevékenysége meg kell feleljen a minősített szolgáltatókra vonatkozó követelményeknek.

Az üzemeltetési tevékenységre figyelembe kell venni a NISZ Zrt. társasági szintű működtetés menedzsment szabályait, és be kell tartani a PKI szolgáltatásokra vonatkozó speciális belső üzemeltetési előírásokat is, a HSZSZ-M szabályzatban leírtak szerint.

A Szolgáltatónak külső fél által ellenőrzött minőségirányítási rendszerrel, továbbá belső információbiztonsági irányítási rendszerrel is rendelkeznie kell.

7.4.6. Hozzáférés menedzsment

A Szolgáltató által kialakított hozzáférés menedzsment meg kell feleljen a minősített szolgáltatókra vonatkozó követelményeknek. Az ezzel kapcsolatos szabályokat részben a Szolgáltató HSZSZ-M szabályzata, részben a belső nem publikus szabályzatai tartalmazzák.

7.4.7. A biztonságos rendszer bevezetése és karbantartása

A biztonságos időbélyegzés szolgáltatás bevezetése és karbantartása érdekében a Szolgáltató.:

- elvégezte az időbélyegzés szolgáltató rendszer, annak fizikai és személyi környezetének kockázatelemzés alapú vizsgálat,
- kidolgozta a szolgáltató rendszer megvalósítása előtt a minősített szint eléréséhez szükséges biztonsági követelményeket,
- biztosította, hogy csak megbízható forrásból származó termékeket és rendszereket használjon, és gondoskodott arról, hogy ezek védve legyenek a jogosulatlan hozzáférésektől és módosításoktól
- a biztonságos rendszer karbantartása a napi operatív, valamint a rendszeres tervezett belső ellenőrzések és külső auditok, az ezek nyomán elvégzett korrekciós, valamit a változásmenedzsment intézkedésekkel történik.

7.4.8. A Szolgáltató kompromittálódása

A Szolgáltató a következő esetekben kompromittálódik:

1. a NISZ Zrt. Főtanúsítványkiadó (Root CA) aláíró kulcsának kompromittálódása,
2. a NISZ Zrt. Minősített Tanúsítványkiadó aláíró kulcsának kompromittálódása
3. az időbélyegzés szolgáltatás valamelyik aláíró kulcsának kompromittálódása,
4. az időbélyegzés szolgáltatás időalap kalibrációjának elvesztése esetén.

Mindegyik esetben az időbélyegzés szolgáltatást fel kell függeszteni mindaddig, amíg új és érvényes aláíró kulcs, tanúsítvány, illetve pontosan kalibrált időalap nem áll rendelkezésre.

A Szolgáltatás internetes honlapján (http://hiteles.gov.hu) tájékoztatni kell az Előfizetőket és felhasználóikat illetve az Érintett feleket a felfüggesztés tényéről és okáról.

Az 1., 2. és 3. kulcs kompromittálódás esetei katasztrófa eseménynek, a 4. eset súlyos üzemzavarnak minősülnek, amelyek kezelésére a Szolgáltató HSZSZ-M szabályzata és a PKI Szolgáltatások Üzletmenet-folytonossági Terve tartalmazza az intézkedéseket.

7.4.9. A Szolgáltató működésének befejezése

A Szolgáltató befejezi működését, ha a NISZ Zrt. tulajdonosa és vezetése ilyen határozatot hoz. A Szolgáltató működése befejezésének oka lehet katasztrófa szintű vagy más esemény is, amelynek következtében megszüntető határozat születik. A Szolgáltató működésének befejezésére a hitelesítés szolgáltatás leállítására vonatkozó jogszabályokat és előírásokat kell betartani, a két szolgáltatás eltérő jellegzetességeinek figyelembevételével.

A Szolgáltató működése felfüggesztésre is kerülhet, ha az NMHH, mint illetékes hatóság felfüggesztő határozatában erről rendelkezik.

7.4.10. Jogszabályoknak való megfelelés

A jogszabályi megfelelés vonatkozásában a 7.1.2 pontnál (Közzétételi nyilatkozat) leírtak az irányadók.

7.4.11. Az időbélyegzés szolgáltatás működtetésével kapcsolatos adatok rögzítése

Az időbélyegzéssel kapcsolatosan a következő adatok kerülnek rögzítésre:

a. az időbélyegzés szolgáltatás fő lépései, a kérelemtől az időbélyeg válasz elküldésig,

b. az időbélyegzés szolgáltatás aláíró kulcsa életciklusában bekövetkező események (generálás, használat, használaton kívül helyezés, visszavonás, megsemmisítés),

c. az időbélyegzés szolgáltatás aláíró kulcs tanúsítványa életciklusában bekövetkező események (kiadás, használat, használaton kívül helyezés, visszavonás).

d. a rögzített adatok a HSZSZ-M 5.4 pontjával összhangban naponta naplózásra és tárolásra kerülnek. A tárolt naplók archiválása a HSZSZ-M 5.5 pontjával összhangban történik. Az archivált adatok megőrzési ideje 10 év.

7.5. Szervezeti séma

Az időbélyegzés szolgáltatásért a NISZ Zrt.-n belül a PKI Ügyfélkapcsolati Iroda az illetékes szervezet, a műszaki rendszer üzemeltetését a NISZ Zrt. belső egységei végzik.

8. Meghatározások és rövidítések

8.1. Meghatározások

A jelen ISZR a 2001. évi XXXV. törvény és a 3/2005. (III. 18.) IHM. rendelet által használt alapfogalmakat használja, amelyek meghatározását a HSZSZ-M 1.6 pontja tartalmazza.

8.2. Alkalmazott jelölések

ÁSZF-PKI: Általános Szerződési Feltételek PKI szolgáltatásokhoz

HSZSZ-M: Szolgáltatási Szabályzat minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz

ISZR: Időbélyegzés Szolgáltatási Rend

NMHH: Nemzeti Média- és Hírközlési Hatóság

UTC: Coordinated Universal Time, az ITU-R TF.460-5 ajánlás szerint definiált, másodperc felbontású időalap